數學傳播　49卷1期, pp. 58-68

Abel 不可約定理及其應用

林開亮

1. 引子: 1939 年的一道題目

近年來, 筆者曾在咸陽、湘潭、武漢、太倉等地給大學一年級數學本科生和高中生做報告, 介紹下列問題的歷史與解法。

問題 1: 已知 $\sqrt{2}+i$ 爲方程式

$$x^6+3x^5-3x^4-6x^3+11x^2+27x-9=0$$

之一根, 求其餘諸根。

報告的部分文字稿及此問題的來源, 詳見 [10, 11]。以下我們先介紹解法。

2. 題目的解答

爲求解問題1, 我們需要方程論中的以下兩個基本結果 (見[6] 中譯本p. 544與 p. 546, 對應於原著 pp. 444–445):

定理 1: (**實係數方程虛根成對**)若一個實係數多項式 $f(x)$ 有虛根, 則這些虛根必定成對出現。也就是說, 若 $a+bi$ (其中 a,b 是實數並且 $b\neq 0$) 是 $f(x)$ 的一個根, 則 $a-bi$ 也是它的根。

定理 2: (**共軛根全部出現**)設 $f(x),p(x)$ 是有理係數多項式, 且 $p(x)$ 在有理數範圍內不可約。若 $p(x)$ 有一個根是 $f(x)$ 的根, 則 $p(x)$ 整除 $f(x)$, 從而 $p(x)$ 的所有根都是 $f(x)$ 的根。

有了定理 1 與定理 2, 即可如下求解問題 1。

解: 根據定理 1, 方程有兩個根 $\sqrt{2}+i$, $\sqrt{2}-i$。

注意到以上兩個根滿足方程

$$x^2-2\sqrt{2}x+3=0.$$

令

$$p(x)=(x^2-2\sqrt{2}x+3)(x^2+2\sqrt{2}x+3)=(x^2+3)^2-(2\sqrt{2}x)^2=x^4-2x^2+9,$$

則不難驗證, $p(x)$ 在有理數範圍內不可約。爲此, 首先注意到 $p(x)$ 的四個根: $\sqrt{2}+i, \sqrt{2}-i, -\sqrt{2}+i, -\sqrt{2}-i$ 都不是有理數, 從而 $p(x)$ 不存在一次有理因式。其次, 爲證明 $p(x)$ 不存在二次有理因式, 只要證明以下六個二次因式都不是有理係數多項式即可:

$$(x-(\sqrt{2}+i))(x-(\sqrt{2}-i)),\ (x-(\sqrt{2}+i))(x-(-\sqrt{2}+i)),\ (x-(\sqrt{2}+i))(x-(-\sqrt{2}-i)),$$

$$(x-(\sqrt{2}-i))(x-(-\sqrt{2}+i)),\ (x-(\sqrt{2}-i))(x-(-\sqrt{2}-i)),\ (x-(-\sqrt{2}+i))(x-(-\sqrt{2}-i)).$$

這是顯而易見的, 它們分別等於

$$x^2-2\sqrt{2}x+3,\quad x^2-2ix-3,\ x^2-2i\sqrt{2}-1,\ x^2-1+2\sqrt{2}i,\ x^2+2ix-3,\quad x^2+2\sqrt{2}x+3.$$

於是, 根據定理 2, $p(x)$ 的所有根都是

$$f(x)=x^6+3x^5-3x^4-6x^3+11x^2+27x-9$$

的根, 這就給出 $f(x)$ 的四個根: $\sqrt{2}+i, \sqrt{2}-i, -\sqrt{2}+i, -\sqrt{2}-i.$ [1]

爲求 $f(x)$ 的另外兩個根, 計算

$$q(x)=\frac{f(x)}{p(x)}=\frac{x^6+3x^5-3x^4-6x^3+11x^2+27x-9}{x^4-2x^2+9}=x^2+3x-1.$$

由二次方程的求根公式, $q(x)$ 的兩根爲 $\frac{-3+\sqrt{13}}{2}$, $\frac{-3-\sqrt{13}}{2}$。

綜上, 方程 $f(x)=0$ 其餘諸根爲:

$$\sqrt{2}-i,\ -\sqrt{2}+i,\ -\sqrt{2}-i,\ \frac{-3+\sqrt{13}}{2},\ \frac{-3-\sqrt{13}}{2}.$$

從以上解法可以看出, 關鍵在於給出 $p(x)$, 然後應用定理 2。

對今天的高中生來說, 定理 2 可能比較陌生。但對當年的高中生來說, 定理 2 是高中數學之基本內容, 因爲當時許多高中都採用 H. B. Fine (1858∼1928) 的《范氏大代數》[6] 作爲教材。

定理 2 會在下一節證明。

3. Abel 不可約定理

定理 2 其實大有來頭, 它可以追溯到 19 世紀的挪威數學家 Niels Abel (1802∼1829)。

事實上, 有以下 Abel 不可約定理 ([4, p. 120]):

定理3: (Abel **不可約定理**)令 $p(x)$ 和 $f(x)$ 是同一個係數體上的多項式, 且 $p(x)$ 有一根是 $f(x)$ 的根。若 $p(x)$ 不可約, 則 $p(x)$ 整除 $f(x)$。特別地, $p(x)$ 的所有根都是 $f(x)$ 的根。

[1]對於學過 Galois 理論的讀者, 也許一眼就可看出 $f(x)$ 的這四個根。參見 [1, p. 38] 命題 15, [2, p. 152] 或 [10]。

注意, 定理 2 是 Abel 不可約定理在係數爲有理數時的特例。

定理 3 中提到“體” (英文 field, 或譯“域”, 德文 körper) 的概念, 它是近世代數中的一個重要概念, 我們略作介紹。

定義 1: 一個集合 F 被稱作體, 是指 F 上面有加法“$+$”與乘法“$\cdot$”運算, 這兩種運算滿足

- 結合律: 對 F 中任意元素 a, b, c, 都有
$$(a+b)+c=a+(b+c), \qquad (a\cdot b)\cdot c=a\cdot(b\cdot c);$$
- 交換律: 對 F 中任意元素 a, b, 都有
$$a+b=b+a, \qquad a\cdot b=b\cdot a;$$
- 分配律: 對 F 中任意元素 a, b, c, 都有
$$(a+b)\cdot c=a\cdot c+b\cdot c;$$
- 存在加法單位元素 0 及乘法單位元素1, 0 與 1 不相等, 使得對 F 中任意元素 a, 都有
$$a+0=a, \qquad a\cdot 1=a;$$
- 存在加法逆元素: 對 F 中任意元素 a, 存在元素 b, 使得
$$a+b=b+a=0;$$
- 對 F 中任意不等於 0 的元素 a, 存在乘法逆元素 c, 使得
$$a\cdot c=c\cdot a=1.$$

簡而言之, 體就是可以做加減乘除四則運算的集合。例如, 有理數的全體構成一個體, 即所謂的有理數體, 通常記爲 $\mathbb{Q}$。所有的實數構成一個體, 即實數體, 記爲 $\mathbb{R}$; 所有的複數構成一個體, 即複數體, 記爲 $\mathbb{C}$。讀者可以驗證, 集合
$$\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\,|\,a,b\in\mathbb{Q}\}$$
構成一個體。

不難發現, 多項式、次數、長除法、因式、公因式等概念, 可以推廣到任何體。

定義 2: 設 F, K 是兩個體, 若 $F\subset K$, 則稱 K 是 F 的擴體。

例如, 由
$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{R}\subset\mathbb{C}$$

可知, 從第二個體開始, 每一個體是前邊所有體的擴體。

定理 3 中提到多項式的根, 實際上要在擴體意義下理解。

定義 3: 設 $f(x)$ 是體 F 上的多項式, K 是 F 的一個擴體, 若 $\alpha \in K$ 使得 $f(\alpha) = 0$, 則稱 α 是 $f(x)$ 在擴體 K 中的一個根 (或零點)。

順便指出, 體論中有一個基本結果說: 若 $f(x)$ 是體 F 上的 n 次多項式, 則存在 F 的擴體 K, 使得 $f(x)$ 在 K 中恰好有 n 個根 (完全分裂)。此處所涉及的精確概念是多項式的分裂體 (splitting field for a polynomial)。

爲證明定理 3, 我們要用到兩個多項式 $f(x), g(x)$ 的最大公因式的 Bézout 等式。照德國數學家 E. Hecke (1887∼1947) 的看法 [9], 這一結果是關於體上的多項式的最重要事實。爲方便讀者, 我們將該定理引述如下。

定理4: 設 $f(x), g(x)$ 是係數體 F 上的兩個非零多項式, 則存在一個可以唯一確定的最大公因式 $d(x)$, 它滿足:

(i) 它在係數體 F 上且首項係數爲 1;
(ii) $d(x) \mid f(x)$ 且 $d(x) \mid g(x)$;
(iii) 每一個同時整除 $f(x)$ 和 $g(x)$ 的多項式也整除 $d(x)$。

並且 $d(x)$ 可以表示爲

$$d(x) = u(x)f(x) + v(x)g(x),$$

其中 $u(x), v(x)$ 是係數體 F 上的多項式。

證明: 先考慮 $f(x), g(x)$ 互質的情形, 令 J 爲所有可以表成 $u(x)f(x) + v(x)g(x)$ 型式的多項式所成的集合, 其中 $u(x)$、$v(x)$ 爲任意多項式。明顯地, $0 \in J$, 且如果 $a(x), b(x) \in J$, 則對任意多項式 $u(x)$, $v(x)$, $u(x)a(x) + v(x)b(x)$ 亦屬於 J (註: 近世代數裡滿足此性質的 J 稱作理想 (ideal))。

設 $d(x)$ 是 J 中非零, 且次數最小的元素, 可以假設其首項係數爲 1。因爲 $f(x), g(x) \in J$, 我們只須證明 J 中任何元素皆是 $d(x)$ 的倍式即可 (由此推出 $d(x)$ 是常數)。

設 $h(x) \in J$, 由長除法得知, 存在多項式 $q(x), r(x)$, 其中或 $r(x) = 0$, 或其次數小於 $d(x)$ 的次數, 使得: $h(x) = q(x)d(x) + r(x)$。但因爲 $h(x) \in J$ 及 $q(x)d(x) \in J$, 從而 $r(x) = h(x) - q(x)d(x) \in J$, 又由次數的假設可知 $r(x) = 0$, 故得證。

一般情況, 令 $d(x)$ 爲 $f(x), g(x)$ 的最大公因式, 因此 $f(x)/d(x), g(x)/d(x)$ 都是多項式, 由上面特殊情況的結論, 可得多項式 $u(x), v(x)$, 滿足 $u(x)f(x)/d(x) + v(x)g(x)/d(x) = 1$, 所以 $u(x)f(x) + v(x)g(x) = d(x)$。證畢。 □

定理 4 有一平行的整數版本。它斷言, 對任意兩個正整數 a, b, 存在整數 u, v 使得 $d = ua + vb$, 其中 $d = \gcd(a, b)$ 是 a, b 的最大公因數 (greatest common divisor)。它可用類似的方法證明 (請讀者自己試證)。這一結果可追溯到 Euclid。並且, 可用 Euclid 算法 (輾轉相除法) 給出這兩個平行結果的構造性證明 (也留給有興趣的讀者)。

定理 3 的證明: 用反證法。若 $p(x)$ 不整除 $f(x)$, 則兩者互質, 故存在多項式 $u(x), v(x)$ 使得

$$u(x)f(x) + v(x)g(x) = 1.$$

但若 α 爲 $p(x), f(x)$ 的公共根, 在上式中令 $x = \alpha$, 就有 $0 = 1$。矛盾! 證畢。 □

4. 應用1: 代數數的極小多項式

定義 4: (**代數數**) 複數 α 稱爲代數數, 若它滿足一個首項係數爲 1 的有理係數多項式方程, 即滿足

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0, \quad \text{其中 } c_{n-1}, \ldots, c_0 \text{ 是有理數。}$$

例如 $\alpha = \sqrt{2}$ 是代數數, 因爲它滿足 $\alpha^2 - 2 = 0$。再如, 每個有理數都是代數數。

一個複數如果不是代數數, 就稱爲超越數。法國數學家 Hermite (1822～1901) 在 1873 年證明了歐拉常數 e 是超越數, 德國數學家 Lindemann (1852～1939) 在 1882 年證明了圓周率 π 是超越數。

有興趣的讀者不妨自己證明:*所有的代數數成一可數的集合* (countable set)。

對給定的代數數 α, 它滿足的有理係數多項式方程顯然不唯一。但可以給出一個最簡單的零化多項式, 它由以下定理刻劃。

定理 5: 設 α 是一個代數數, 則存在唯一的有理係數多項式 $p(x)$ 滿足以下條件:

(i) $p(x)$ 首項係數爲 1;
(ii) $p(\alpha) = 0$;
(iii) 若有理係數多項式 $f(x)$ 使得 $f(\alpha) = 0$, 則 $p(x) \mid f(x)$。

證明: 存在性。考慮以 α 爲根的所有首項係數爲 1 的有理係數多項式全體, 其中必有一個次數最低, 令它爲 $p(x)$。根據 Abel 不可約定理, 爲證明 $p(x)$ 的極小性質 (iii), 只要證明 $p(x)$ 不可約。這是顯然的, 因爲若

$$p(x) = p_1(x)p_2(x),$$

其中 $p_1(x), p_2(x)$ 是首項係數爲 1 的次數更低的有理係數多項式, 則從 $p(\alpha) = 0$ 推出 $p_1(\alpha) = 0$ 或 $p_2(\alpha) = 0$, 從而與 $p(x)$ 的次數最低矛盾!

唯一性。設 $p(x), q(x)$ 都滿足定理所述條件, 則由 $p(x)$ 的極小性質得到 $p(x) \mid q(x)$, 由 $q(x)$ 的極小性質得到 $q(x) \mid q(x)$。從而我們有 $p(x) = cq(x)$。由於 $p(x), q(x)$ 的首項係數爲 1, 我們得到 $c = 1$, 從而 $p(x) = q(x)$。證畢。 $\square$

以上定理引出下述定義[2]:

定義5: (**代數數的極小多項式、次數與共軛**) 定理 5 中給出的唯一多項式稱爲代數數 α 的極小多項式。給定代數數 α, 我們稱其極小多項式的次數爲 α 的次數, 稱其極小多項式的全部根爲 α 的共軛。

根據定理 5 的證明, 我們知道, 代數數的極小多項式是不可約的有理係數多項式。並且我們還知道, 若代數數 α 的次數爲 n, 則它恰好有 n 個不同的共軛。(想一想, 爲什麼?)

例如, 對 $\alpha = \sqrt{2}$, 它的極小多項式爲 $x^2 - 2$, 共軛爲 $\sqrt{2}, -\sqrt{2}$。再如, 對有理數 r, 其極小多項式爲 $x - r$, 僅有平凡的共軛 r。

在基體爲有理數體的情況, 借助代數數和共軛的概念, Abel 不可約定理可以重新表述如下:

定理6: (**共軛根定理**)若代數數 α 是有理係數多項式 $f(x)$ 的根, 則 α 的共軛都是 $f(x)$ 的根。

現在我們回看問題 1 的解法, 其關鍵就在於, 對代數數 $\alpha = \sqrt{2} + i$, 求出了它的極小多項式 $p(x)$ 及其共軛 $\sqrt{2}+i, \sqrt{2}-i, -\sqrt{2}+i, -\sqrt{2}-i$。

以下結果, 也許在中學就有模糊的認識而未經證明, 這裡我們留作習題。

定理7: (**無理根定理**)設係數皆爲有理數之方程式有一根 $a + \sqrt{b}$, 其中 a, b 爲二有理數, $\sqrt{b}$ 爲一無理數。則此方程式有一根 $a - \sqrt{b}$。

對給定的代數數, 求它的極小多項式與共軛, 是一個重要的問題, 我們在下一節介紹一些經典的結果。

值得指出, 代數數的概念可以推廣到任何體上面, 給定一個體 F 及其擴體 K。我們稱 K 中的元素 α 是“F 上的代數數”, 若且唯若 α 是某個係數在 F 中的首項係數爲 1 的多項式的根。有興趣的讀者不妨自證以下命題:

- *F 上的每個代數數皆有極小多項式。*
- *若α是F上的代數數, 且其極小多項式的次數爲 n, 則 K 中所有可以表成 $g(\alpha)$ 的元素, 此*

[2]從近世代數的眼光看, α 的極小多項式可以這樣描述。賦值映射 $f(x) \mapsto f(\alpha)$ 給出一個從多項式環 $F[x]$ 到 $F[\alpha]$ 的一個環同態 ϕ, 它的核 $\mathrm{Ker}(\phi) = \{f(x) \in F[x] : f(\alpha) = 0\}$ 是 $F[x]$ 的一個理想。由於 $F[x]$ 的每個理想是主理想 (principal ideal), 從而存在 $p(x) \in F[x]$, 使得 $\mathrm{Ker}(\phi) = (p(x))$。若要求 $p(x)$ 首項係數爲 1, 則它是唯一的。由於 $p(x)$ 不可約, 我們由環同態基本定理還得出 $F[\alpha]$ 是一個體。這個事實是 Abel 首先認識到的, 見 [2, p. 80]。

$g(x)$ 爲係數在 F 裡且次數小於 n 的多項式, 構成一體。

- K中所有 F 上的代數數構成一體。
- 若 $F=\mathbb{R}$, 則所有的複數都是 F 的代數數, 其極小多項式的次數是 1 或 2。

5. 一些常見的代數數

這裡我們介紹三類常見的代數數及其極小多項式和共軛。

5.1. 質數次方根$\sqrt[p]{a}$

無理數 $\sqrt{2}$ 的一個簡單推廣是質數次方根 $\sqrt[p]{a}$, 這裡 p 是質數, 且 a 是有理數且 a 不是任意有理數的 p 次方。

先看一個具體的例子: $\sqrt[3]{2}$。它是 $x^3-2=0$ 的唯一實根。容易看到, $\sqrt[3]{2}$ 的極小多項式就是 $x^3-2=0$, 而其共軛則是 $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2$, 其中 ζ 是一個三次本原單位根 (本原單位根的一般概念將在下文介紹)。

一般地, 若 a 是有理數且 a 不是任意有理數的 p 次方, 其中 p 是某個給定的質數, 則 $\sqrt[p]{a}$ 的極小多項式是 x^p-a, 其共軛爲 $\sqrt[p]{a}\zeta^k$, $0\leqslant k\leqslant p-1$, 其中 ζ 是一個 p 次本原單位根。這裡關鍵的結果是以下可以追溯到 Abel 的定理 (參見 [2, pp. 86–87]):

定理8: (Abel–Kronecker **定理**) 設 p 是質數。則體 F 上的多項式 x^p-a 在 F 中可約當且僅當 $a=b^p$, 這裡 $b\in F$。

證明: 若 $a=b^p$, 則

$$x^p-a=x^p-b^p=(x-b)(x^{p-1}+bx^{p-2}+\cdots+b^{p-1}).$$

下證, 若 x^p-a 在 F 中可約, 則 $a=b^p$, 這裡 $b\in F$。

設 $f(x)$ 是係數體 F 上的一個 ℓ 次多項式 (這裡 $1\leqslant\ell\leqslant p-1$), 首項係數爲 1, 且滿足 $f(x)\mid x^p-a$。於是$f(x)$ 的所有根 $r_1,\ldots,r_\ell$ 都滿足 $r^p=a$, 從而 $f(0)^p=((-1)^\ell r_1\cdots r_\ell)^p=((-1)^\ell)^p a^\ell$. 這意味著 $a^\ell=f(0)^p((-1)^\ell)^p=((-1)^\ell f(0))^p$。由於 $1\leqslant\ell\leqslant p-1$, 從而 p,ℓ 互質, 於是根據定理 4 的整數平行版本, 存在整數 u,v 使得 $1=up+v\ell$, 從而

$$\begin{aligned}a=a^{up+v\ell}&=(a^u)^p(a^\ell)^v=(a^u)^p(((-1)^\ell f(0))^p)^v=(a^u)^p(((-1)^\ell f(0))^v)^p\\&=(a^u((-1)^\ell f(0))^v)^p.\end{aligned}$$

令 $b=a^u((-1)^\ell f(0))^v$, 即得 $a=b^p$。證畢。 □

5.2. 單位根 ζ

在所有的二項多項式 $x^n - a$ 中, 以 $x^n - 1$ 形式上最簡單。$x^n - 1$ 在複數體上的根, 稱爲 n 次單位根 (nth roots of unity)。顯然, 一共有 n 個 n 次單位根, 可以用指數 (或三角函數) 表示爲

$$e^{i\frac{2k\pi}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right),\ 0 \leqslant k \leqslant n-1.$$

它們恰好對應著將單位圓周 n 等分的 n 個分點。

設 ζ 是一個 n 次單位根, 若對任意的 $1 \leqslant m \leqslant n-1$, ζ 都不是 m 次單位根, 則稱 ζ 是一個本原 n 次單位根 (primitive nth root of unity)。容易驗證, 一個 n 次本原單位根具有形式

$$e^{i\frac{2k\pi}{n}} = \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right),\ 0 \leqslant k \leqslant n-1 \text{且 } k, n \text{ 互質。}$$

遵循 Euler, 我們以 $\varphi(n)$ (稱爲 Euler 函數) 表示集合 $\{1, \ldots, n-1\}$ 中與 n 互質的整數的個數, 則 n 次本原單位根一共有 $\varphi(n)$ 個。例如, 對於質數 p, $\varphi(p) = p-1$。

若 $n \geqslant 2$, 則顯然 $x^n - 1 = (x-1)(x^{n-1} + \cdots + 1)$ 在有理數體可約。

1772 年, Euler 首先給出了 $x^n - 1$ 在有理數體上的一個因式分解 (後來才表明這是不可約因式分解):

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

注意, $\Phi_n(x)$ 可以從上式遞迴算出, 例如令 $n = 1$, 即得 $\Phi_1(x) = x - 1$, 而對一切 $n > 1$, 有

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n,\\ d<n}} \Phi_d(x)}.$$

特別地, 對於 $n = p$ 是質數的情況, 有

$$\Phi_p(x) = \frac{x^p - 1}{\prod_{\substack{d|p,\\ d<p}} \Phi_d(x)} = \frac{x^p - 1}{\Phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + 1.$$

$\Phi_n(x)$ 稱爲第 n 個分圓多項式 (cyclotomic polynomial), 它的零點恰好是所有的 n 次本原單位根, 這是由 Gauss 首先明確指出的:

$$\Phi_n(x) = \prod_{\substack{1 \leqslant k \leqslant n\\ \gcd(k,n)=1}} (x - \zeta_n^k), \quad \text{其中 } \zeta_n = e^{i\frac{2\pi}{n}}.$$

1801年, Gauss 首先證明了, 對質數 p, 第 p 個分圓多項式 $\Phi_p(x)$ 不可約[3]。由此可知, 對於 p 次本原單位根 $\zeta_p = e^{i\frac{2\pi}{p}}$, 它的極小多項式是 $\Phi_p(x) = x^{p-1} + \cdots + 1$, 其次數是 $p-1$,

[3]後來德國數學家 T. Schönemann(1812∼1868) 與 G. Eisenstein (1823∼1852) 先後給出了更簡潔的證明, 參見 [3]。

ζ_p 的共軛是全部的 p 次本原單位根, 即 ζ_p^k, $1 \leqslant k \leqslant p-1$。請讀者自行導出 $n=p^m$ 的分圓多項式。

1854 年, 德國數學家 Kronecker (1823∼1891) 證明了, 對任意的正整數 n, 第 n 個分圓多項式 $\Phi_n(x)$ 不可約。由此即得以下定理:

定理9: 設 $\zeta_n = e^{i\frac{2\pi}{n}} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, 則它的極小多項式是第 n 個分圓多項式 $\Phi_n(x)$, 其次數是 $\varphi(n)$, ζ_n 的共軛是全部的 n 次本原單位根, 即 ζ_n^k, $0 \leqslant k \leqslant n-1$ 且 k, n 互質。

將 Gauss 引向 n 次本原單位根的, 是用尺規作圖將圓周 n 等分的問題。Gauss 在 1801 年出版的《算術探索》[7] 最後一章最後一節指出: 用尺規作圖可以將圓周 n 等分當且僅當 $\varphi(n)$ (注意它是 n 次本原單位根的次數) 是 2 的一個方冪[4]。特別地, Gauss 發現可以用尺規作圖將圓周 17 等分 ($\varphi(17)=16=2^4$)。

1837年, 受 Gauss 這一工作的啟發, 法國數學家 Pierre Wantzel (1814∼1848) 解決了尺規作圖三大著名難題中的兩個, 他證明了用尺規作圖不可倍立方, 用尺規作圖不可三等分任意角。前者的關鍵在於 $\sqrt[3]{2}$ 的次數爲 3, 不是 2 的一個冪。後者實際上可歸結爲 Gauss 的前述結果, 因爲 60° 可以尺規作圖三等分當且僅當單位圓可以用尺規作圖 9 等分, 而根據 Gauss 的結果, $\varphi(9)=6$ 不是 2 的冪, 是不可以用尺規作圖 9 等分的。

應該指出, 正是 Gauss 關於分圓方程 $\Phi_p(x)=0$ 的先驅工作, 啟發了 Abel 和 Galois 關於方程論的偉大工作。

5.3. 有理角的三角函數

從 Euler 等式

$$e^{i\theta} = \cos\theta + i\sin\theta$$

不難得到

$$2\cos\theta = e^{i\theta} + e^{-i\theta}.$$

從而我們可以從 n 次本原單位根 $e^{i\frac{2\pi}{n}}$ 的資訊得到 $2\cos\frac{2\pi}{n}$ 的信息。基本結果如下。

令 $2\cos\frac{2\pi}{n}$ 的極小多項式爲 $\Psi_n(x)$, 則 $\Psi_1(x)=x-2$, $\Psi_2(x)=x+2$, 而當 $n \geqslant 3$ 時, $\Psi_n(x)$

$$\frac{\Phi_n(x)}{x^{\frac{\varphi(n)}{2}}} = \Psi_n(x+x^{-1}), \tag{1}$$

其中 $\varphi(n)$ 如前爲 Euler 函數。據此, 從 $\Phi_n(x)$ 可算出 $\Psi_n(x)$。$\Psi_n(x)$ 稱爲第 n 個實分圓多項式。

[4]根據這一結果, 對於 $n=2,3,4,5,6,8,10,12$, 可以用尺規作圖將圓周 n 等分。而 $n=7,9,11$ 的情況, 則無法用尺規作圖從圓周得到正 n 邊形。這也解釋了, 爲何在許多建築中, 我們能見到正三角形、正方形、正五邊形、正六邊形、正八邊形等, 而很少見到正七邊形、正九邊形和正十一邊形等。參見 [12]。

根據定義, 有

$$\frac{\Phi_n(x)}{x^{\frac{\varphi(n)}{2}}} = \frac{\prod\limits_{\substack{1\leqslant k\leqslant n\\ \gcd(k,n)=1}} (x-\zeta_n^k)}{x^{\frac{\varphi(n)}{2}}} = \prod_{\substack{1\leqslant k\leqslant \frac{n}{2}\\ \gcd(k,n)=1}} \frac{(x-\zeta_n^k)(x-\zeta_n^{n-k})}{x}$$
$$= \prod_{\substack{1\leqslant k\leqslant \frac{n}{2}\\ \gcd(k,n)=1}} \left(x+x^{-1}-2\cos\frac{2k\pi}{n}\right).$$

進而有

$$\Psi_n(x) = \prod_{\substack{1\leqslant k\leqslant \frac{n}{2}\\ \gcd(k,n)=1}} \left(x-2\cos\frac{2k\pi}{n}\right).$$

5.4. 有理角的三角函數

俄國大數學家 I. M. Gelfand (1913~2009) 與合作者 A. Shen 在其爲中學生寫的《代數》教材 [8, p. 67] 中曾給出一個因式分解的例題:

$$\begin{aligned} x^5+x+1 &= x^5+x^4+x^3-x^4-x^3-x^2+x^2+x+1\\ &= x^3(x^2+x+1)-x^2(x^2+x+1)+(x^2+x+1)\\ &= (x^3-x^2+1)(x^2+x+1). \end{aligned}$$

作者還緊忙評論道:“也許你被這個解答弄得垂頭喪氣, 因爲它似乎不可能被看出來。作者與你感同身受。” 事實上, 對於 x^5+x+1 的因式分解, 利用 Abel不可約定理, 立即可以發現它有因式 x^2+x+1。我們留給有興趣的讀者探究。

致謝

感謝西北農林科技大學劉昌勇教授、湖南大學李軍教授、湘潭大學孫鵬教授、學友吳帆老師與作者討論交流。感謝首都師範大學李克正教授、北京師範大學劉玉明教授、中央民族大學王兢教授、中國礦業大學 (北京) 張漢雄教授和本刊審稿老師對初稿提出寶貴意見。

参考文獻

1. E. Artin, *Galois Theory*, Dover, 1998. 有中譯本, 李同孚譯,《伽羅瓦理論》, 哈爾濱工業大學出版社, 2011。
2. D. A. Cox, *Galois Theory*, Pure and Applied Mathematics (2nd ed.), John Wiley & Sons, 2012.

3. D. A. Cox, Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first, *Amer. Math. Monthly*, 118(1) (2011), 3–21.
4. H. Dörrie , *100 Great Problems of Elementary Mathematics: Their History and Solution*, Dover, 1965. 有中譯本, 羅保華等譯,《100個著名初等數學問題: 歷史和解答 》, 上海科學技術出版社,1982。
5. H. M. Edwards, Galois for 21st-century readers, Notices Amer. Math. Soc. 59 (2012), no. 7, 912–923. 有中譯文, 馮緒寧譯《21世紀的讀者閱讀 Galois》,《數學譯林》, 2013。
6. H. B. Fine, *A College Algebra*, Boston: Ginn & Co, 1905. 中譯本《新編範氏代數》, 楊大淳等編譯, 科學出版社, 1983。
7. C. F. Gauss, *Disquisitiones Arithmeticae*, translated by A. A. Clarke, Springer, 1986. 中譯本《算術探索》, 潘承彪、張明堯譯, 哈爾濱工業大學出版社, 2011。
8. I. M. Gelfand, A. Shen, *Algebra*, Boston: Birkhäuser, 1993. 中譯本,《代數》, 胡長青、麻希南譯, 中國科學技術大學出版社, 2020。
9. E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Math., vol. 77, Springer-Verlag, Berlin and New York, 1981. 中譯本《代數數理論講義》, 王元譯, 北京, 科學出版社, 2005。
10. 林開亮。Abel-Galois 不可約原理漫談: 從劉昌勇老師的問題談起。好玩的數學, 2023-07-01。
11. 林開亮。Abel-Galois 不可約原理。好玩的數學, 2023-11-08。
12. 石勇國。商周太陽神鳥金飾中蘊含的數學文化。《數學通報》, 2020卷59卷12期, 54-56。

—本文作者任教中國西北農林科技大學理學院—